WORLD **PRIVACY** FORUM

October 1, 2009

Bobbie Holm, Chief, Policy Branch
California Privacy and Security Advisory Board
California Health and Human Services Agency
California Office of Health Information Integrity
1600 9th Street
Room 460
Sacramento, CA 95814

Dear Ms. Holm,

The World Privacy Forum appreciates the opportunity to respond to the letter of dissent AHIP submitted to the CalPSAB board. In the letter, AHIP mentioned the World Privacy Forum had voted nay on the CalPSAB's consent motion. This is correct. We did cast a nay vote, and this letter more fully articulates the reasons why we cast that vote.

Additionally, we would like to respond to the overarching argument in the AHIP letter that HIPAA should be the primary basis of the board's decision-making process regarding health information exchange policies and procedures in the state of California.

First, we would like to more fully explain our nay vote on opt-out. Essentially, the motion concerned whether or not Californians should have to opt-out of health information exchange for treatment purposes, or opt-in. The majority of the board voted that Californian's should have to opt-out of health exchange. In other words, the default position would be that Californians' health care records will be exchanged for treatment purposes, unless an individual actively opted out, with some potential exceptions to be more fully determined in December.

The World Privacy Forum as a consumer representative on the board voted nay because the preponderance of the research, the case studies, the HIE and NHIN pilot projects, and the technology all indicate that in this transitional time, when HIE is just getting established, that opt in is a better and safer choice for consumers. Opt in will encourage consumer trust, will improve public health, build long-term sustainability of the HIE systems, and will protect vulnerable populations.

It is crucial to remember that this opt in does not change an individual's ability to get healthcare treatment; it determines the default position of information exchange with

other entities. It is also crucial to remember that patients do have the choice to opt in, and that providers may acquire an opt in from patients.

The opt-out approach contains numerous risks for consumers and for healthcare providers. Our carefully considered opinion is that opt in for electronic exchange of healthcare records is the best mitigation solution for consumers at this point in time.

The Chilling Effect on Patient Care

The nation's most respected healthcare policy advisory body is the National Committee on Vital and Health Statistics (hereafter NCVHS.) This committee was tasked with creating recommendations for the National Health Information Network (hereafter NHIN). The NCVHS spent years in a serious and deliberative process collecting expert testimony from all stakeholders and holding numerous hearings throughout the country to gather input. This body has issued significant and respected recommendations about health information exchange and the NHIN.

The NCVHS has already logged many thoughtful hours and hearings on the consent and opt-in/opt-out issue regarding health information exchange (hereafter HIE). One of the most challenging issues they tackled was the chilling effect HIE could have on public health and on patient care due to the presence of sensitive or stigmatizing information in patient files. This is not a perspective that has come up very much in the CalPSAB board meetings, in part due to light consumer participation. But when there is representation from a large variety of consumer stakeholders, as was the case with NCVHS, this is quickly revealed as a core issue and concern in HIE.

In discussion about the NHIN, Dr. Mark Rothstein, co-chair of the NCVHS Privacy and Confidentiality subcommittee, articulated how sensitive information in health care records can lead to multiple challenges in an electronic environment. He said:

> I think there is a real public health issue here, and there is a lot of literature in the public health world that people will forgo, delay, abandon treatment for mental illness, STDs, anything that has a stigma attached to it if they have no confidence that they can control that information. In the paper world, the unconnected world, I could go to a STD clinic or maybe my college health service to be treated for a STD. Now in the electronic interconnected world, it doesn't matter where I go because presumably all of that will be connected. Unless there is some sort of way that patients can have confidence that treatment for their most sensitive sort of conditions, drug problems or what have you, is not going to be routinely disclosed to every subsequent requester – then I worry.[1]

The American College of Obstetricians and Gynecologists gave thoughtful testimony about this issue, noting:

---

[1] Department of Health and Human Services National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentiality Working Session, June 19, 2007, transcript.

> Patient approval of electronic recordkeeping within the confines of a physician's office should not necessarily imply that patients would be as agreeable to other information-sharing, such as availability of information through the NHIN. Accordingly, ACOG also strongly supports the NCVHS recommendations that individuals should have a choice about whether to participate in the NHIN and that providers should not be able to condition treatment on an individual's agreement to have his or her health records accessible via the NHIN. …Keeping participation voluntary also will minimize and public health concerns regarding patients' refusal to seek treatment for a condition because of a fear the records will become public.[2]

The core issue relates to sensitive information. It was not a surprise when Dr. Simon Cohn, chairman of the NCVHS wrote to then-Secretary Leavitt that "**Individual control of sensitive health information is one of the most important privacy issues to be resolved in developing and implementing the NHIN**."[3]

The state of California has a strong interest in encouraging individuals to seek prompt treatment for health conditions, including those conditions which may have a stigma attached to them such as HIV-AIDS, substance abuse, mental health, sexual assault, domestic violence, and even genetically-linked diseases. If individuals fear the stigmatizing information may not be in their control, they may delay treatment or avoid it altogether. We want to avoid this outcome for Californians, and for HIE.

Segregation of Data as a Key Mitigation Tool

Through NCVHS' work and through the many NHIN pilot and demonstration projects, it has become clear that a key mitigation strategy for handling sensitive information in health records is segregation of that data. The general lines of the policy thinking is that by addressing the sensitive information issue, the stigma issue is removed, and the public health issues and chilling effect issues are thereby mitigated. This is the position the NCVHS came to in 2008, when it made its formal policy recommendation of data segregation in the NHIN:

> NCVHS recommends enhancing the privacy protections of individual health information by affording individuals limited control over disclosure of sensitive health information among their health care providers via the NHIN. We believe this approach is compatible with improving the quality of health care, promoting patient trust in the health care system, and safeguarding public health.[4]

---

[2] Testimony of Dr. Robert J. Fagnant, on behalf of the American College of Obstetricians and Gynecologists before the National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentiality, April 17, 2007.

[3] Simon P. Cohn, Chairman, NCVHS. Letter to Michael O. Leavitt, February 20, 2008.

[4] *Id*.

The NCVHS also noted that there should be exceptions to this for emergency treatment, which we agree with.

But there are some significant technical challenges right now with data segregation. Generally, the technology has not advanced to the point where data segregation is workable to the degree it needs to be in order to be effective. One of the most significant challenges in this area is the issue of intermingled records. The NCVHS has discussed this issue, noting that, for example, that substantial amounts of mental health records considered sensitive can be found in primary care physician files containing prescriptions for Valium, etc. Under the treatment category, all of the information can be exchanged, and there is little to no ability to fully and consistently reliably segregate all of the sensitive information out of health care files at this time.

The need for segregation of sensitive categories of information should not be minimized – important consumer privacy interests exist in this area. For example, a victim of domestic violence is very unlikely to want to have her records shared outside of her immediate treatment. This is reasonable. Victims of domestic violence face tangible harm if their records get into the wrong hands, which is why substantive laws such as the Violence Against Women Act already exist that strongly protect information and files relating to this vulnerable population.

Other intangible harms exist, such as shame or embarrassment. Patients should have the right to make a decision about whether or not their information, particularly their sensitive information, goes out beyond their immediate circle of treatment. Because the technology does not yet support segregation of sensitive information to the levels that are required, then the only position that is left for vulnerable populations is the opt-in option. This option, at this time in the development of technology, allows individuals with genuine needs or desires for appropriate information segregation to protect themselves and their health care records proactively.

The worst-case scenario here is a patient who, after the fact, finds out his or her records have been exchanged, and because of that, they now have a safety or other problem related to that wider dissemination.

We have not focused here on the legal risks of an opt-out approach. We have read the CalPSAB Legal Committee's analysis of the legal risks of an opt-out approach, and agree that an opt-out approach may ultimately lead to lawsuits against providers that did not appropriately control patient data or adequately inform patients of data exchanges.

We have also not focused here on medical identity theft victims. We note for the record that victims of medical identity theft who have their incorrect records exchanged become vulnerable to improper treatment. We have already seen many of these cases, and are

deeply concerned about what happens to these victims when their records are exchanged without an express opt-in.[5]

Navigating the Middle Ground

The World Privacy Forum believes that the middle ground for California is to take a transitional approach to HIE. We see that technology will ultimately enable sequestration of sensitive information. When this occurs, opt-out with opt-in for sensitive data will make much more sense. But until then, opt-in across the board is the least risky and safest approach.

The Need to Go Beyond HIPAA

We would like to briefly respond to the AHIP letter regarding the importance of relying on HIPAA as a primary standard for developing California's HIE policies. First, many non-HIPAA covered entities will be involved with HIE. We note that FERPA-covered entities may well end up participating in HIE. We also note that gyms, direct-to-consumer testing companies, and a large variety of other non-covered entities may participate in HIE. HIPAA leaves too many parties out of the HIE equation. It is not appropriate to make HIPAA the sole primary standard for HIE, when HIPAA did not contemplate protecting information in such a structure.

The NCVHS recommended that HHS should "work with other federal agencies and the Congress to ensure that privacy and confidentiality rules apply to all individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, application service providers and schools."[6] The NCVHS was in particular concerned that:

> Many of the new entities essential to the operation of the Nationwide Health Information Network fall outside HIPAA's statutory definition of "covered entity." Health information exchanges, regional health information organizations, record locator services, community access systems, system integrators, medical record banks, and other new entities established to manage health information have proliferated in recent years.[7]

---

[5] For more background on medical identity theft, see World Privacy Forum, Medical Identity Theft: The Information Crime That Can Kill You, May 2006. < http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf>

[6] Recommendation R-12. Dr. Simon P. Cohn, Chairman, NCVHS. Letter to Secretary Leavitt Re: Update to privacy laws and regulations required to accommodate NHIN data sharing practices, June 21, 2007.

[7] Dr. Simon P. Cohn, Chairman, NCVHS. Letter to Secretary Leavitt Re: Update to privacy laws and regulations required to accommodate NHIN data sharing practices, June 21, 2007.

HIE represents a new way of doing things, and as such new rules need to be crafted and applied to appropriate entities. Congress expressly recognized this in its 2009 ARRA legislation. In the legislation, the Federal Trade Commission was given unprecedented authority to undertake a rulemaking impacting health care records held by commercial PHR vendors due to concerns about protection of medical data held outside of HIPAA.[8] We view these statutes and rulemakings as appropriate and reasonable responses that help provide meaningful protections for consumers in a rapidly evolving health care sector.

Thank you for this opportunity to articulate our views regarding these important issues. The World Privacy Forum appreciates the thoughtful efforts that state has undertaken to determine a pathway forward in HIE policy. The decisions we arrive at now will have far-reaching consequences in the future. Our greatest concern is that the consumers of California achieve the maximum benefit HIE has to offer while being protected from the risks such a system by its nature introduces. We believe these risks can be mitigated by a thoughtful opt-in approach at this point in time.

Sincerely,

Pam Dixon
Co-Chair, CalPSAB
Executive Director, World Privacy Forum

---

[8] See 16 C.F.R. Part 318, Health Breach Notification Rule. Final Rule -- Issued Pursuant to the American Recovery and Reinvestment Act of 2009 -- Requiring Vendors of Personal Health Records and Related Entities To Notify Consumers When the Security of Their Individually Identifiable Health Information Has Been Breached. < http://www2.ftc.gov/os/2009/08/R911002hbn.pdf>.